UNITED STATES DISTRICT COURT

for the

Western District of Virginia

United States of America
v.
Ioana-Cristina Pavel

Case No. 7:19MJ120

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of April 13, 2019 through May 5, 2019 in the county of Botetourt in the Western District of Virginia, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1029(a)(1)	Access Device Fraud
18 U.S.C. § 1028A	Aggravated Identity Theft

This criminal complaint is based on these facts:

See Attached Affidavit

☑ Continued on the attached sheet.

Complainant's signature

Angelo Rella, Agent, U.S. Secret Service
Printed name and title

Sworn to before me and signed in my presence.

Date: September 20, 2019

Judge's signature

City and state: Roanoke, Virginia

Hon. Judge Robert S. Ballou
Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST WARRANT

Introduction

I, Angelo M. Rella, being duly sworn, depose and state as follows:

1. I am the Senior Resident Agent of the Roanoke Resident Agency with the United States Secret Service. I have been employed by the United States Secret Service for twenty two years. The Secret Service has a dual mission, we provide protection for the President, Vice President, their families, former presidents, presidential candidates, visiting foreign heads of state, National Special Security Events and others as directed by Congress or lawful authority. In addition, we also conduct criminal investigations related to financial crime. These investigations include counterfeit currency, credit card/access device fraud, telecommunications fraud, check fraud, bank fraud, crimes against children, mortgage fraud and cybercrime (network intrusions, phishing, auction fraud, romance scams, foreign lottery scams, etc.). Throughout my career I have conducted numerous investigations related to counterfeit currency, credit card fraud, telecommunications fraud, check fraud, cybercrimes, crimes against children and cybercrime.

2. This criminal complaint is being submitted in support of a criminal complaint and arrest warrant charging Ioana-Christina Pavel with Access Device Fraud in violation of Title 18, United States Code, Section 1029(a)(1) and Aggravated Identity Theft in violation of Title 18, United States Code, Section 1028A.

3. I have participated in the investigation leading to the information contained in this affidavit both through personal investigation as well as through discussions with other law enforcement personnel. This affidavit contains information necessary to support probable cause. The information contained in this affidavit is not intended to include each and every fact known to the United States.

Definitions

4. **"Personal Identifying Information (PII)"** includes all means of identification which may be used alone or with other information to identify a specific individual, such as a credit card account number or a driver's license number, as well as any other unique personal identifying information.

5. **"Access device"** means any card, account number, personal identification number, or other means of account access which can be used, alone or in conjunction with another access device, to obtain money, goods, services or other things of value, or can be used to initiate a transfer of funds.

6. **"Counterfeit Access Device"** means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device. The term "cloned card" as used herein would be considered a counterfeit access device.

7. **"Means of identification"** means any name or number that may be used, alone, or in conjunction with any other information, to identify a specific individual, including any unique electronic identification number.

8. **"A Personal Identification Number,"** commonly called PIN, is a number assigned by the issuing financial institution to be used in conjunction with a credit card or debit card in order to facilitate financial transactions at a point of sale (POS) or at an Automatic Teller Machine (ATM). A PIN number is typically a unique number assigned to the cardholder only and not written or engraved on the corresponding card.

Factual Background

9. In May 2019, the United States Secret Service (USSS) Roanoke Resident Agency started an investigation into a credit card skimming organization. The investigation was

prompted by reports from multiple local law enforcement agencies in southwest Virginia that numerous victims filed complaints of unauthorized ATM withdrawals from their bank accounts.

10. Through this investigation it was discovered that beginning on an unknown date no later than on or about March 12, 2019 and continuing through May 5, 2019, Ioana-Christina Pavel (hereinafter "Pavel") and others known and unknown to the United States, worked together to fraudulently obtain personal identifying information (PII), including debit/credit card numbers and corresponding PINs, from bank customers without lawful authority and used that data to make unauthorized cash withdrawals from the accounts of these victims and/or use the victims' credit for their personal gain.

11. Specifically, Pavel and others known and unknown to the United States utilized access device making equipment, commonly referred to as "skimming devices" to facilitate this scheme. They installed these devices, along with small hidden cameras (referred to as pinhole cameras), without authorization, onto ATM machines to capture victims' means of identification including bank account numbers and PINs. The skimmer is inserted deep into the card reader and is not visible to the victim when they insert their debit/credit card. The pinhole camera is similarly hidden/disguised out of view but at an angle allowing it to capture the victim's PIN as they continue with their transaction. The skimmer captures the information on the magnetic stripe on the back of the victim's card. This information is then re-encoded onto counterfeit or cloned cards. These cards are then used in conjunction with the stolen/captured PINs to make unauthorized withdrawals from victim accounts.

12. Through this investigation, after multiple discussions with local law enforcement investigators, bank investigators and surveillance video review, it was discovered that Pavel and others placed "skimming devices" on ATMs in Henry County (VA), Vinton (VA), Montgomery

County (VA), Campbell County (VA), Roanoke County (VA), Roanoke City (VA), Appomattox County (VA), Rocky Mount (VA), Mars Hill (NC), Sophia (WV) and Raleigh County (WV). The locations referenced above in Virginia are all located within the Western Judicial District of Virginia.

13. While installing these devices, on several occasions, Pavel and others attempted to conceal their identity (facial covering, hats, glasses, facial hair) or otherwise obscure the video surveillance (covering the camera with their hands or opaque object). Their methods of operation varied with respect to the placement or removal of "skimming devices."

14. They then recovered the "skimming devices" and pinhole cameras and used the data captured to create fraudulent or altered access devices, commonly referred to as re-encoded or cloned cards. They then used these fraudulent access devices, in conjunction with the victims' PINs to steal money from bank accounts through ATM machines. With respect to Pavel, the details surrounding some of her specific actions, including her arrest on state charges, are set forth below.

15. On May 5, 2019, the Botetourt County Sheriff's Office received a citizen complaint regarding possible fraudulent activity at a Bank of Fincastle ATM located at 614 Lee Highway, Roanoke, Virginia. This bank and ATM are located within the Western Judicial District of Virginia. The caller, Victim M.D., waited at the bank for the Botetourt Sheriff's Deputy to respond so that he could report a prior unauthorized fraudulent withdrawal from his wife's HomeTrust bank account connected to her debit card. While he waited, Victim M.D. observed a white female with long black hair wearing a baseball cap standing at the outer most drive thru ATM. Victim M.D. stated the female acted suspiciously, attempted to hide her face, quickly departed the ATM, and walked to a blue vehicle parked across the street behind a bush. Victim

M.D. reported this activity to the Sheriff's Office and provided a description of the vehicle, including its New York license plates, and the direction of travel.

16. Deputy Faulkner with the Botetourt County Sheriff's Office observed a vehicle matching the description provided by victim M.D. and began surveillance. As he observed the vehicle, Deputy Faulkner saw one of the occupants litter as he observed what appeared to be a small red bag being thrown out of the vehicle. He further observed the vehicle accelerate very rapidly on the wet road surface and as a result it lost traction. Based upon these observations and the information previously provided Deputy Faulkner initiated a traffic stop. The vehicle was occupied by a male driver (Farkas P. Szilard) and a female passenger (Pavel). Both Szilard and Pavel initially denied being at the bank or using the ATM. Szilard later stated he used the ATM to withdraw $200.00. Deputy Faulkner questioned the occupants regarding the woman with long black hair reported by victim M.D. Szilard and Pavel denied knowing anything about a woman with long black hair. Due to the rain, Deputy Faulkner requested Szilard step out of the car and onto the porch of a derelict house for further questioning. Deputy Davis had Pavel step out of the vehicle and sit in the rear of his patrol vehicle. At this time, in plain view on the floorboard of the passenger seat where Pavel sat, Detective Jody Edwards observed a black long hair wig and a dark colored baseball cap.

17. During the questioning of the occupants, two Botetourt Sheriff's deputies arrived at the Bank of Fincastle where victim M.D. had reported the suspicious activity. There they reviewed the ATM security footage of the suspicious incident. Szilard and Pavel were observed using multiple cards to make multiple withdrawals. They were then arrested and taken into custody. The vehicle was towed and a state search warrant was obtained. The search of the vehicle resulted in the recovery of the following items (not an inclusive list):

a. $8,800 in US currency, the majority recovered were $20.00 bills consistent with ATM withdrawals. Romanian currency was also discovered along with a receipt for a wire transfer.

b. Bag with makeup and hats and a head wrap.

c. 46 Panera gift cards re-encoded (cloned) with debit/credit card account information of victims' accounts with a hand-written four digit PIN affixed to each re-encoded card.

d. Materials and components used to manufacture deep insert skimmers, pin hole cameras and related equipment such as flat stock, SD cards, hand tools, double sided tape, metallic sheets, metal file and sand paper.

e. Numerous articles of clothing, wallets and purses that appeared similar or matched clothing, wallets and purses observed on Pavel and others in her group in ATM and other surveillance videos. These items were matched at the time of the traffic stop and during subsequent investigation and review of additional surveillance video.

18. Subsequent investigation and review of ATM surveillance video revealed Pavel and others made or attempted to make multiple unauthorized and fraudulent withdrawals at various Bank of Fincastle ATMs located in the Western Judicial District of Virginia. It was discovered that the victim bank accounts from which they made or attempted to make these withdrawals had been compromised by "skimming device" equipment installed at the Farmers Bank of Appomattox, 10272 Village Highway, Concord, VA; Farmers Bank of Appomattox, 169 Old Courthouse Rd, Appomattox, VA; HomeTrust Bank, 5002 Williamson Road NW, Roanoke, VA and at United Bank, 425 Robert C. Byrd Drive, Sophia, West Virginia.

19. Pavel was captured on ATM surveillance video conducting or attempted to conducting the following unauthorized transactions at various Bank of Fincastle locations using the cloned cards (counterfeit access devices) and stolen PINs. The debit/credit card associated with the compromised bank account is listed first, followed by the address for the Bank of Fincastle where the withdrawal occurred/was attempted, and followed by the amount of United States currency withdrawn. For each of these transactions Pavel knew she was not the account

holder and that she did not have the account holder's authorization to use their means of identification.

April 13, 2019:

Farmers Bank of Appomattox debit/credit card ending in 7902 was used without authorization at 1245 Roanoke Road, Daleville, VA to withdraw $500.00 USD.

Farmers Bank of Appomattox debit/credit card ending in 8632 was used without authorization at 1245 Roanoke Road, Daleville, VA to withdraw $500.00 USD.

Farmers Bank of Appomattox debit/credit card ending in 9841 was used without authorization at 1245 Roanoke Road, Daleville, VA to withdraw $250.00 USD.

Farmers Bank of Appomattox debit/credit card ending in 8711 was used without authorization at 1245 Roanoke Road, Daleville, VA to withdraw $350.00 USD.

April 28, 2019
United Bank debit/credit card ending in 2175 was used without authorization at 1245 Roanoke Road, Daleville, VA to withdraw $500.00 USD.

United Bank debit/credit card ending in 9927 was used without authorization at 1245 Roanoke Road, Daleville, VA to withdraw $300.00 USD (first transaction with this cloned card).

United Bank debit/credit card ending in 9927 was used without authorization at 1245 Roanoke Road, Daleville, VA to withdraw $100.00 USD (second transaction with this cloned card).

United Bank debit/credit card ending in 9927 was used without authorization at 1245 Roanoke Road, Daleville, VA to withdraw $100.00 USD (third transaction with this cloned card).

United Bank debit/credit card ending in 6719 was used without authorization at 5192 Lee Highway, Troutville, VA to withdraw $300.00 USD.

United Bank debit/credit card ending in 0403 was used without authorization at 5192 Lee Highway, Troutville, VA to withdraw $300.00 USD.

May 4, 2019
HomeTrust Bank debit/credit card ending in 3383 was used without authorization at 5192 Lee Highway, Troutville, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 8212 was used without authorization at 5192 Lee Highway, Troutville, VA to withdraw $230.00 USD.

HomeTrust Bank debit/credit card ending in 6315 was used without authorization at 5192 Lee Highway, Troutville, VA to withdraw $300.00 USD.

HomeTrust Bank debit/credit card ending in 4633 was used without authorization at 5192 Lee Highway, Troutville, VA to withdraw $400.00 USD.

HomeTrust Bank debit/credit card ending in 7511 was used without authorization at 5192 Lee Highway, Troutville, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 6842 was used without authorization at 5192 Lee Highway, Troutville, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 7127 was used without authorization at 5192 Lee Highway, Troutville, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 4595 was used without authorization at 614 Lee Highway, Roanoke, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 0583 was used without authorization at 614 Lee Highway, Roanoke, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 0769 was used without authorization at 614 Lee Highway, Roanoke, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 6948 was used without authorization at 614 Lee Highway, Roanoke, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 7268 was used without authorization at 614 Lee Highway, Roanoke, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 9667 was used without authorization at 614 Lee Highway, Roanoke, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 3633 was used without authorization at 1245 Roanoke Road, Daleville, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 6704 was used without authorization at 1245 Roanoke Road, Daleville, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 1583 was used without authorization at 1245 Roanoke Road, Daleville, VA to withdraw $500.00 USD.

May 5, 2019

HomeTrust Bank debit/credit card ending in 9754 was used without authorization at 614 Lee Highway, Roanoke, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 4862 was used without authorization at 614 Lee Highway, Roanoke, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 7511 was used without authorization at 614 Lee Highway, Roanoke, VA to withdraw $500.00 USD.

HomeTrust Bank debit/credit card ending in 6842 was used without authorization at 614 Lee Highway, Roanoke, VA to withdraw $380.00 USD.

HomeTrust Bank debit/credit card ending in 7460 was used without authorization at 614 Lee Highway, Roanoke, VA to withdraw $500.00 USD.

Attempts Declined on May 4 and 5, 2019

On May 4, 2019, HomeTrust Bank debit/credit card ending in 1977 was used without authorization at 614 Lee Highway, Roanoke, VA. An attempt to withdraw $0.00 USD was declined.

On May 4, 2019, HomeTrust Bank debit/credit card ending in 5515 was used without authorization at 614 Lee Highway, Roanoke, VA. An attempt to withdraw $0.00 USD was declined.

On May 4, 2019, HomeTrust Bank debit/credit card ending in 3821 was used without authorization at 1245 Roanoke Road, Daleville, VA. An attempt to withdraw $0.00 USD and a subsequent attempt to withdraw $500 USD were declined.

On May 5, 2019, HomeTrust Bank debit/credit card ending in 6604 was used without authorization at 614 Lee Highway, Roanoke, VA. Two attempts to withdraw $500.00 USD were declined.

On May 5, 2019, HomeTrust Bank debit/credit card ending in 6325 was used without authorization at 614 Lee Highway, Roanoke, VA. An attempt to withdraw $500.00 USD was declined.

20. Transactions involving HomeTrust Bank and Farmers Bank of Appomattox bank accounts are processed through a company called Fiserv that is located at 11380 Technology Circle, Johns Creek, GA. All ATM transactions route through these servers. HomeTrust Bank also has their headquarters at 10 Woodfin Street, Asheville, North Carolina and all support and customer transaction disputes are processed through the bank's headquarters. Farmers Bank of Appomattox reissued 11,040 debit/credit cards as a result of the skimming incidents. The cards

are issued by third party vendor, Fiserv Output Solutions, payment sent out of state to 75 Remittance Drive, Suite 6943, Chicago, IL. Farmers Bank of Appomattox also contacted Diebold Nixdorf to service their ATMs as a result of this activity. Diebold Nixdorf is located at 5995 Mayfair Rd, North Canton, Ohio. Payment for this service sent to P.O. Box 643543, Pittsburgh, Pennsylvania. The means of identification and PINs associated with the United Bank transactions were obtained at a United Bank in Sophia, West Virginia. All told the information above indicates that the actions of Pavel and her group affected interstate or foreign commerce.

21. Pavel has also been identified as a suspect in additional area fraud reports after being captured on surveillance video at ATMs located in Farmville, Appomattox and Concord, Virginia using re-encode/cloned cards to withdraw money from victim's bank accounts. The investigation into her actions and the actions of other members of her group are still ongoing.

Request for Complaint and Arrest Warrant

For the above-stated reasons, I believe there is probable cause to conclude the following:

22. Beginning on an unknown date no later than on or about March 12, 2019 through May 5, 2019, and others known and unknown to the United States knowingly and with the intent to defraud, produced, used or trafficked in one or more counterfeit access devices, in a manner affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(l).

23. Beginning on an unknown date no later than on or about March 12, 2019 through May 5, 2019 Ioana-Christina Pavel and others known and unknown to the United States knowingly and with the intent to defraud used, without lawful authority, and in a manner affecting interstate commerce, a means of identification of another person, namely PIN numbers and debit/credit card account numbers belonging to unwitting victims, during and in relation to

the felony violation of Access Device Fraud, in violation of Title 18 United States Code, Section 1028A.

Respectfully submitted,

Angelo M. Rella
Senior Resident Agent
U.S. Secret Service

Subscribed and sworn to before me on September 20th, 2019:

UNITED STATES MAGISTRATE JUDGE